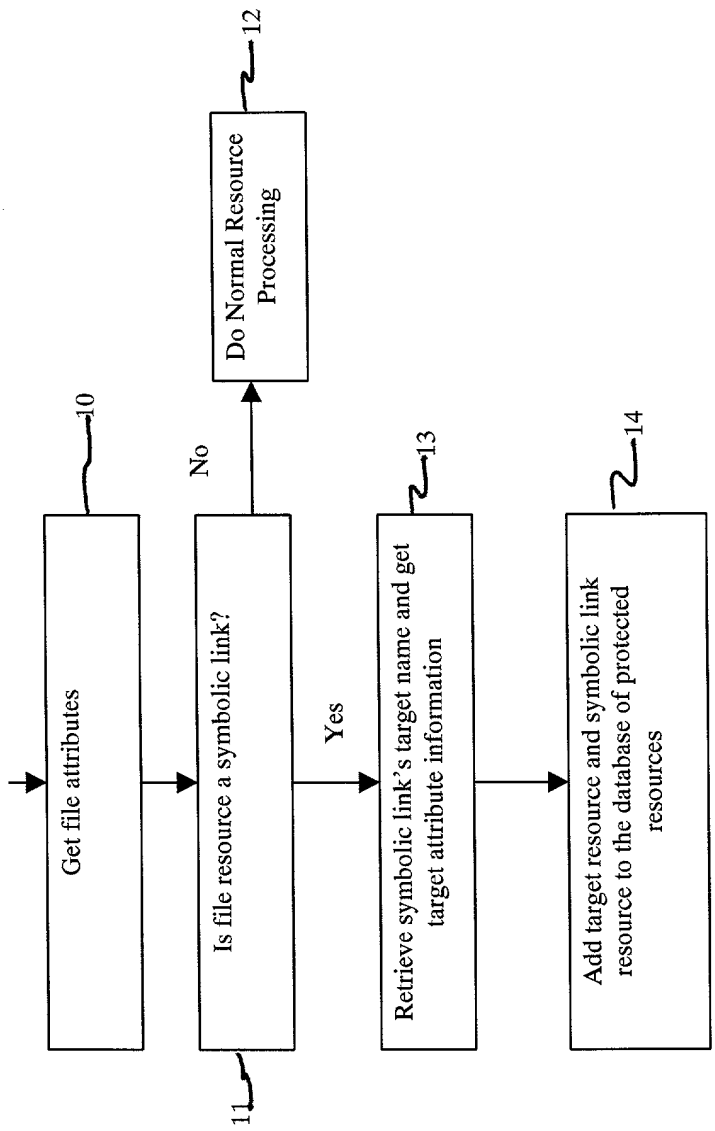

Get file attributes
10
Is file resource a symbolic link?
11
No
Do Normal Resource Processing
12
Yes
Retrieve symbolic link's target name and get target attribute information
13
Add target resource and symbolic link resource to the database of protected resources
14

Figure 1

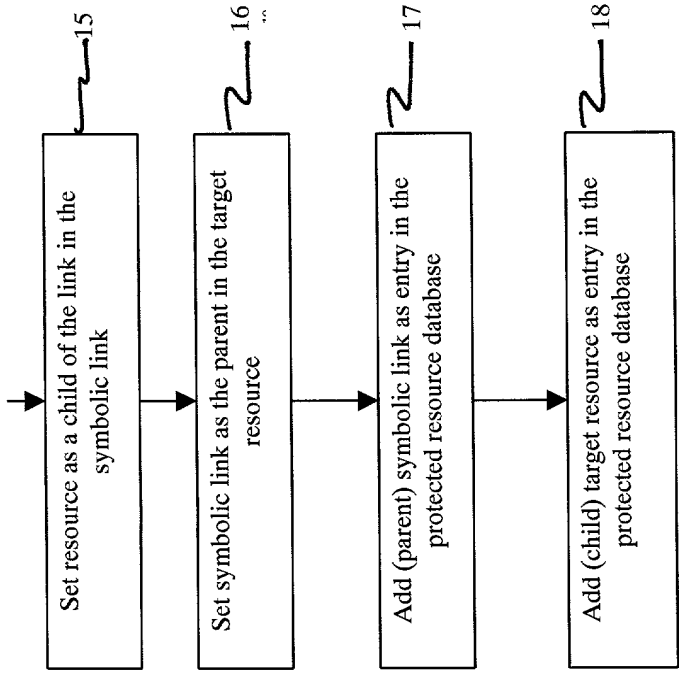

Set resource as a child of the link in the symbolic link
15
Set symbolic link as the parent in the target resource
16
Add (parent) symbolic link as entry in the protected resource database
17
Add (child) target resource as entry in the protected resource database
18

Figure 2

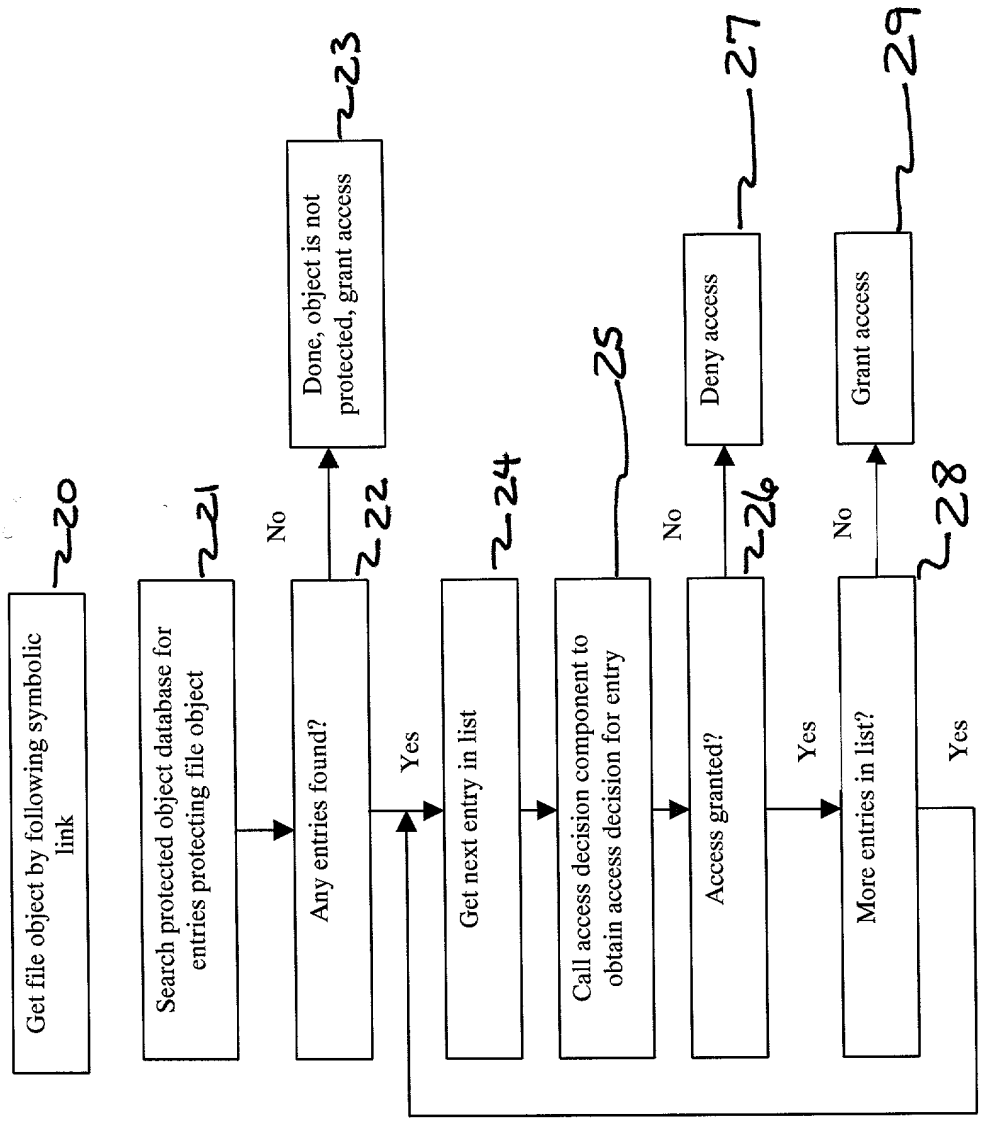

Get file object by following symbolic link
20
Search protected object database for entries protecting file object
21
Any entries found?
22
No
Done, object is not protected, grant access
23
Yes
Get next entry in list
24
Call access decision component to obtain access decision for entry
25
Access granted?
26
No
Deny access
27
Yes
More entries in list?
28
No
Grant access
29
Yes

Figure 3

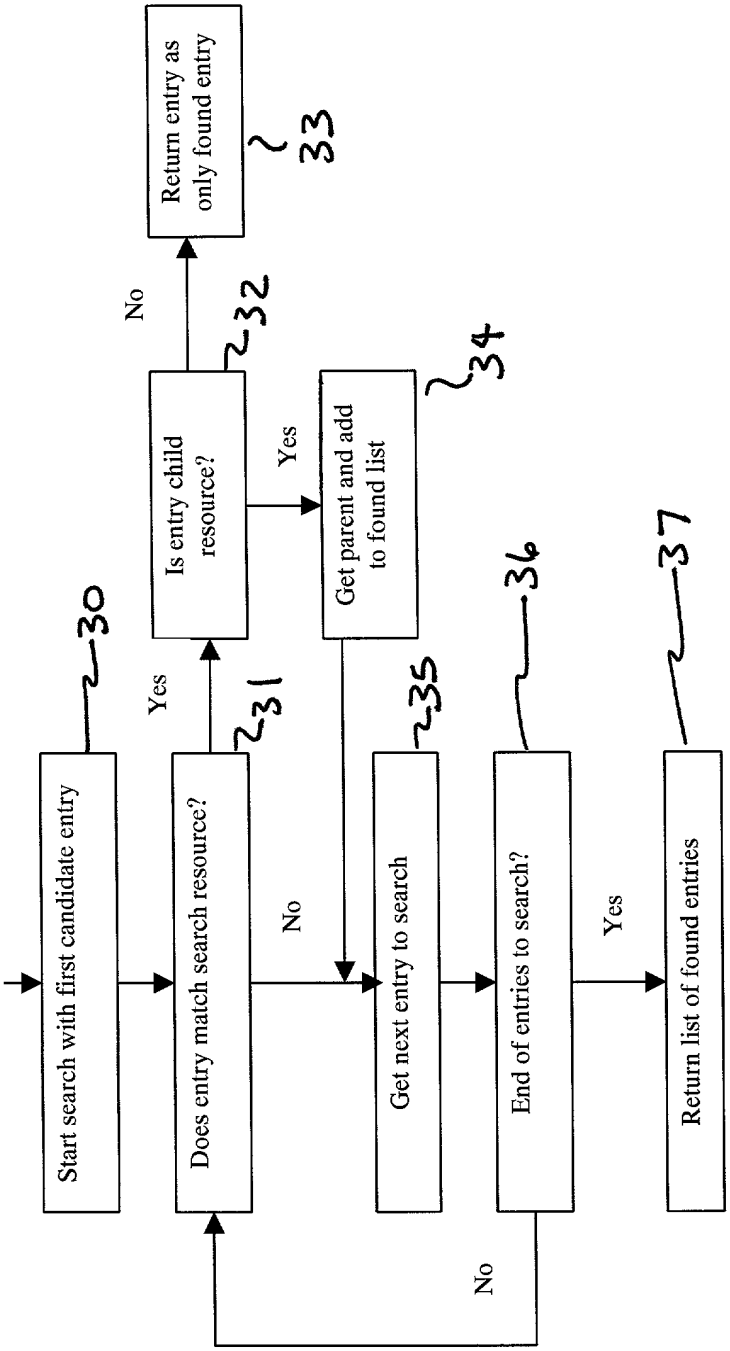

Start search with first candidate entry
30
Does entry match search resource?
231
Yes
No
Is entry child resource?
232
Yes
No
Return entry as only found entry
233
Get parent and add to found list
234
Get next entry to search
235
End of entries to search?
236
No
Yes
Return list of found entries
237

Figure 4

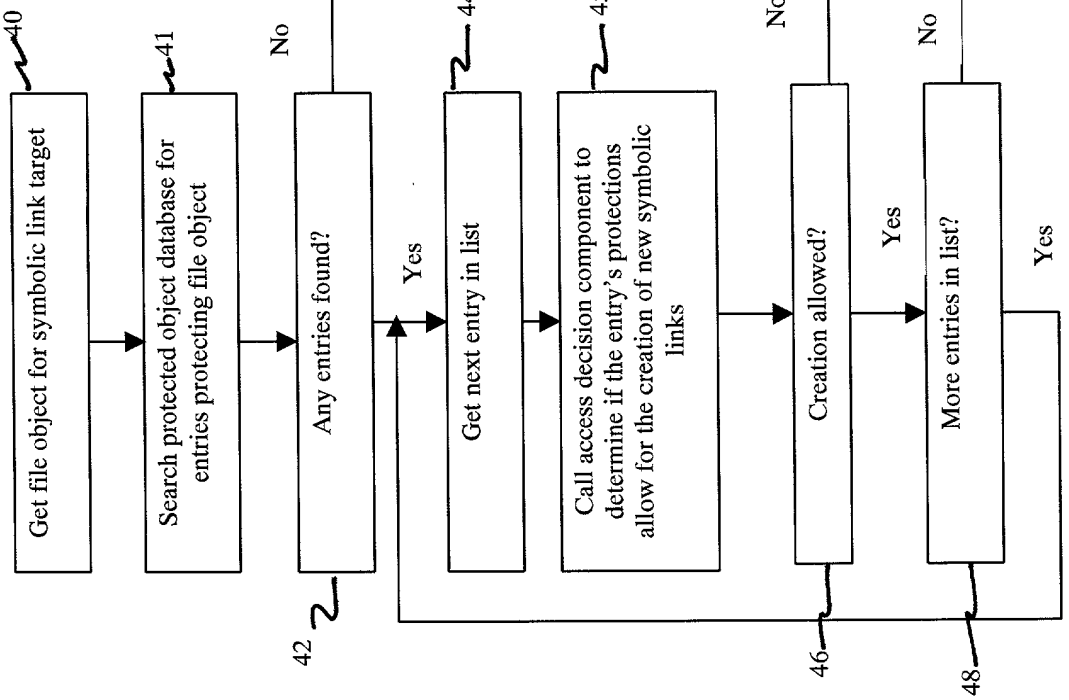

Get file object for symbolic link target
40
Search protected object database for entries protecting file object
41
Any entries found?
42
No
Done, object is not protected, allow create
43
Yes
Get next entry in list
44
Call access decision component to determine if the entry's protections allow for the creation of new symbolic links
45
No
Creation allowed?
46
Deny create
47
Yes
More entries in list?
48
No
Allow create
49
Yes

Figure 5

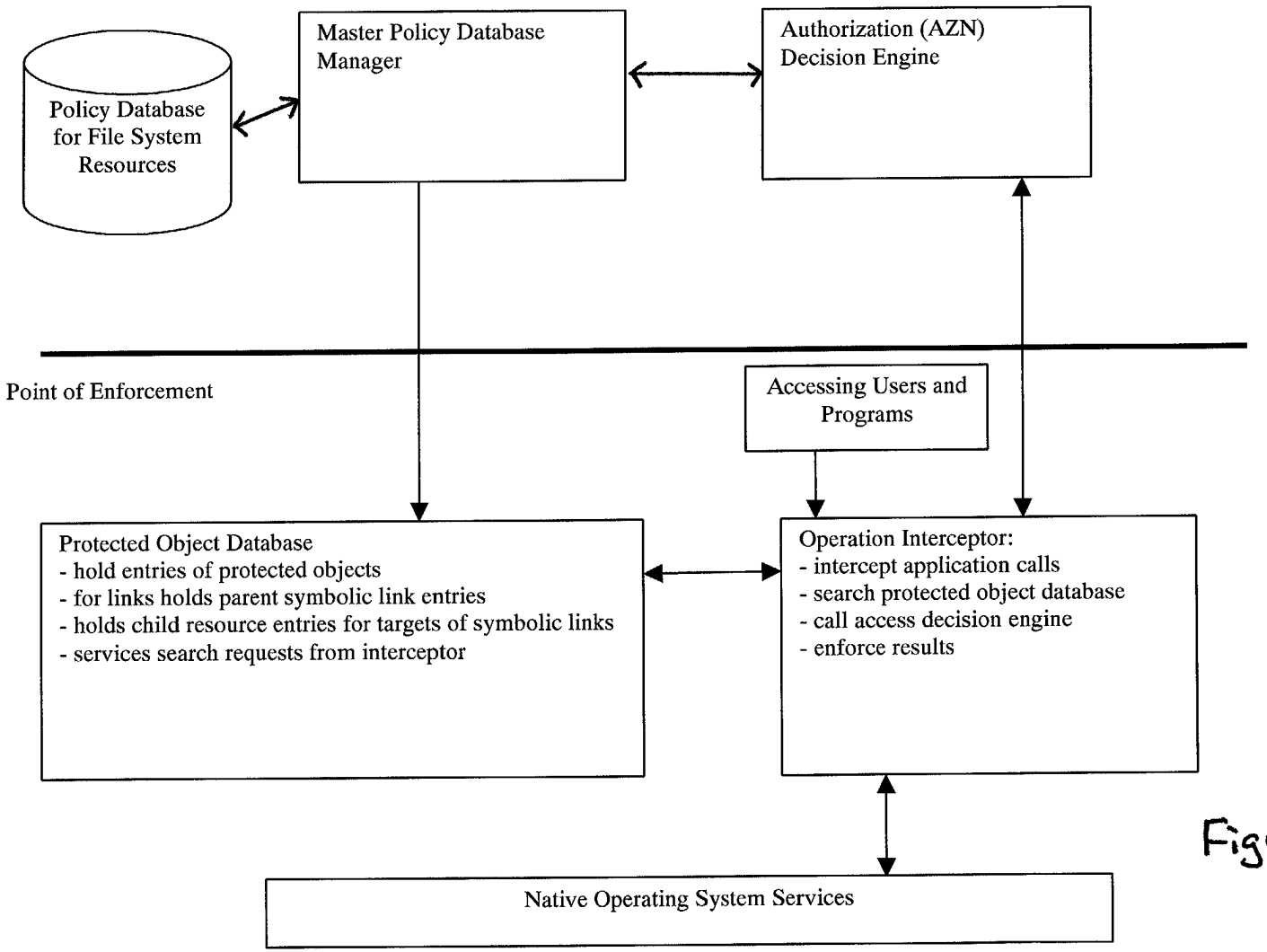
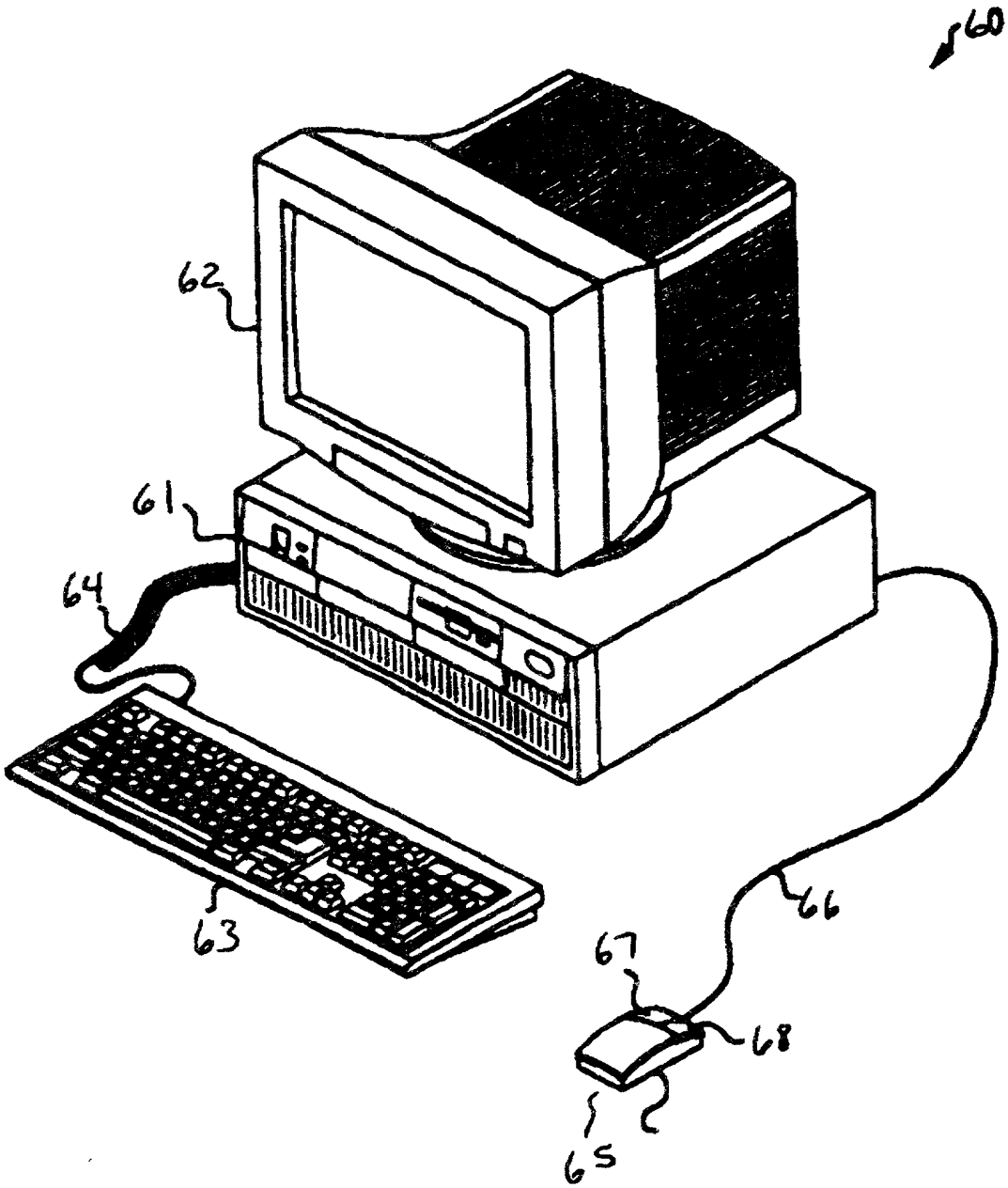

Policy Database for File System Resources
Master Policy Database Manager
Authorization (AZN) Decision Engine
Point of Enforcement
Accessing Users and Programs
Protected Object Database
- hold entries of protected objects
- for links holds parent symbolic link entries
- holds child resource entries for targets of symbolic links
- services search requests from interceptor
Operation Interceptor:
- intercept application calls
- search protected object database
- call access decision engine
- enforce results
Native Operating System Services

Figure 6


60
62
61
64
63
66
67
68
65